OTCnet System Requirements and Reference Guide

OTCnet Release 2.0

Contents

System and Configuration Requirements

This document provides system and configuration requirements for the use of OTCnet Online for deposit processing and check processing/ check scanning. This document also provides system and configuration requirements for OTCnet Offline, which is available for users performing check processing/check scanning in areas with low bandwidth and/or unreliable internet connectivity. The following changes are in the Release 2.0 System Requirements document:

- Other Requirements
- Java 8 Compatibility

OTCnet General Requirements

This section details the system and configuration requirements necessary to utilize all OTCnet functionality. Additional requirements are necessary for OTCnet check processing/check scanning. Refer to the "OTCnet Check Processing Requirements" and "OTCnet Offline Check Capture Application Requirements" sections on the next page for more information.

Operating System

The following operating systems are supported by OTCnet:

- Windows XP (restricted to 32-bit for OTCnet)
- Windows Vista (restricted to 32-bit for OTCnet)
- Windows 7 (OTCnet supports both 32-bit and 64-bit versions of the operating system)

System Requirements

The following are requirements necessary to operate OTCnet:

- **Web Browser**: Internet Explorer 7[1], 8 or 9, 32-bit version only.
  - **Compatibility View or Browser Mode**: If using IE9, Compatibility View must be used or the Browser Mode must be set to IE8 when accessing OTCnet. Users working in Compatibility View or IE8 Browser Mode may see minor formatting differences (borders, shading, link location, etc.) that do not affect OTCnet functionality. Further information is provided below in the Technical Reference Guide.
  - **Zoom:** Must be set at the web browser default (100% zoom). Please note that if zoom is not set to 100%, you may experience issues while using the OTCnet application.
  - **Trusted Site Zone:** The link treas.gov needs to be added to your Trusted Site Zone to log in to the OTCnet application at all times.
- **Entrust Root Certificate:** The Entrust (2048) Root Certificate must be installed in the "Trusted Root Certification Authorities" certificate store on the "local machine" (all user profiles) for the workstation. This certificate is normally installed by default with Internet Explorer. If it has been removed, you will need to have your agency re-install the certificate.
- **Internet Options Security Settings**:
  - "**Use TLS 1.0**" must be enabled in the Advanced tab of Internet Options for all user profiles on the workstation. OTCnet and ITIM are secure websites that require a compatible secure transport protocol to be enabled in the browser.
    - Although OTCnet is also compatible with other settings such as "**Use SSL 3.0**" and "**Use TLS 1.2**", ITIM is currently only compatible with TLS 1.0. As a result, the "**Use TLS 1.0**" setting must be enabled in order to access both ITIM and OTCnet from the same browser.
    - "**Use SSL 2.0**", "**Use SSL 3.0**", "**Use TLS 1.1**" and **"Use TLS 1.2**" may also be enabled if any of these settings are required for other applications or web sites.
- **Ports**: Router/Firewall Administrators must ensure and verify that outbound ACL (Access Control List) has complete https access, on port 443.
- **Workstation Memory**: 2 GB physical memory is required; 4 GB is recommended.
- **Free Disk Space**: 20 MB of free disk space is required.
- **Window Resolution**: Windows Resolution should be 1024x768 or 800x600.

[1] Internet Explorer 7 is not supported on Windows 7

Other Requirements

- **Email Address**: Users must have access to a unique email address to change their initial OTCnet passwords and access the online system.
- **Microsoft Word:** Several OTCnet Reports are made available in RTF file format. If your terminal has Microsoft Word installed, the reports display correctly and are properly formatted; however, if your agency does not have Microsoft Word and you open the reports in a default program such as Wordpad, the reports are not formatted properly.

OTCnet Check Processing Requirements

This section outlines additional requirements necessary to perform OTCnet check processing/check scanning. **These requirements are only necessary if OTCnet is utilized for check processing/check scanning.**

Additional System Requirements

The following system requirements are necessary for utilizing OTCnet check processing. Please note that these requirements must be performed by a Windows administrator (a user who is logged onto the workstation as a workstation administrator):

- **Treasury Root Certificate:** The Treasury Root Certificate must be installed in the "Trusted Root Certification Authorities" certificate store on the "local machine" (all user profiles) for the workstation. Instructions for obtaining and installing the Treasury Root Certificate can be found on the Fiscal Service OTCnet homepage under the OTCnet Onboarding Toolkit.
- **OTCnet URLs Added to Trusted Sites Zone**: OTCnet URLs must be assigned to the Trusted Sites zone for Windows Vista and Windows 7 for all user profiles on the workstation. Note that this requirement is not necessary for Windows XP workstations. Instructions for adding OTCnet URLs to the trusted sites zone is provided below in the Technical Reference Guide.
- **ActiveX must be enabled in browser**: This must be enabled for all user profiles on the workstation that use OTCnet. ActiveX is typically enabled in the Trusted Sites Zone. If it is not enabled in the Trusted Sites Zone or if the OTCnet URLs cannot be added the Trusted Sites Zone, ActiveX will need to be explicitly enabled. Instructions for enabling ActiveX are provided below in the Technical Reference Guide.
- **ActiveX Filtering must be disabled in browser (IE9 only):** If using IE9 (in Compatibility View or IE8 Browser Mode), ActiveX Filtering must be disabled. Further information is provided below in the Technical Reference Guide.
- **Scanner Drivers (.MSI installation file):** Scanner driver and Firmware (provided in an .MSI installation file) must be installed on the workstation. Instructions for obtaining and installing the .MSI file will be provided in a separate document. Further information is provided below in the Technical Reference Guide.
- **Java Runtime Environment (JRE), 32-bit:** The Java Runtime Environment (Java SE 6, Java SE 7, or Java SE 8) must be installed and enabled on the workstation.

  It is recommended that the latest release of Java 8, 32-bit be maintained at all times to ensure the highest level of security and OTCnet Check Capture functionality for your workstations. To access information about the latest release of Java 8, click on the following link: http://www.oracle.com/technetwork/java/javase/downloads/index.html, and scroll to the section listing the latest Java 8 release. Please reference your agency's internal policies and procedures prior to taking any action.

  Please note that Java 6 is no longer supported by Oracle and is no longer receiving new security updates. The content of some of the Java updates may cause issues and/or inconsistencies with some browser/workstation combinations and OTCnet check scanning. The chart below shows results of our latest Java compatibility testing.

Java Versions Compatibility					
	Java Version	Operating System			
		Windows XP	Windows Vista	Windows 7	Windows 7
Java 6	1.6.0_0 to 1.6.0_45	Compatible[1]	Compatible[1]	Compatible[1]	Compatible[1]
Java 7	Older Versions of Java 7	Limited Compatibility[1,2]	Limited Compatibility[1,2]	Limited Compatibility[1,2`]	Limited Compatibility[1,2]
	Latest Version of Java 7	**Compatible**	**Compatible**	**Compatible**	**Compatible**
Java 8	Latest Version of Java 8	**Not Compatible**[3]	**Compatible**	**Compatible**	**Compatible**

[1] You may be prompted to accept security warnings to continue using OTCnet when using an older version of Java.
[2]The Java security slider in the Java Control Panel may need to be set to **Medium** for these Java versions for OTCnet to function properly.
[3]Oracle does not support Java 8 on XP; testing has shown that OTCnet is not compatible with Java 8 on XP.

Security Update Installers – Security Update Installer 1.2.0 & OTCnet Security Update January 2014
Agencies installing OTCnet Offline Release 1.4 after March 14, 2014 need to install the repackaged Release 1.4 Offline software, titled OTCNET-1.4.0, and the Security Update Installer- 1.2.0.

Java Expiration Dates
To improve Java security, Oracle has implemented an automatic "expiration" of the current Java version whenever a new release with security vulnerability fixes becomes available. The current Java version will automatically expire with the release of the next critical patch update. For systems without connectivity to Oracle Servers via the internet, a secondary mechanism containing a hard coded expiration date retires the previous version of Java one month after the latest scheduled critical patch update is released.

After a new release becomes available or a hard coded expiration date is reached, Java will provide additional warnings and reminders to users to update to the newest version. For information on Java security resources, please visit: http://www.java.com/en/security/

- **Adobe: All versions of Adobe are compatible with OTCnet, although Adobe X may require web browser configuration changes.**
- **Adobe Reader: Adobe Reader must be installed on the workstation to support receipt printing. All versions of Adobe are compatible with OTCnet, although Adobe X may require web browser configuration changes. Adobe Reader Version 7.x or higher is required.**

Check Processing Hardware Requirements

The following hardware requirements are necessary for utilizing OTCnet check processing:

- Access to a printer from the workstation where you will be using OTCnet for Check processing
- A compatible check scanner connected to the workstation with an available 9-Pin Serial Port, PC Card Slot, or USB 2.0 port
- The following table lists the check scanners that are compatible with OTCnet. The table also indicates which version of the scanner driver and Firmware is required for each combination of scanner and operating system. Blacked out cells indicate INCOMPATIBLE scanner and operating system combinations.

Firmware Version by Scanner and Operating System				
Scanners		Operating Systems		
Scanner Type	Model	XP	Vista[5]	Windows 7
RDM	EC7000i [2, 3]	1.5.1 or 1.6.0	1.5.1	1.5.1 or 1.6.0
	EC9000i	1.6.0		1.6.0
Panini	MyVisionX [4]	1.6.0	1.6.0	1.6.0
	VisionX [4]	1.6.0	1.6.0	1.6.0
	Panini I: Deal	1.6.0	1.6.0	1.6.0

[1] Supported connection via COM (male) to Serial (female)
[2] Supported connection via USB (male) to USB (male) or COM (male) to Serial (female)
[3] Keypad connection requires the use of Firmware 1.5.1 for EC7000 scanners
[4] Panini MyVisionX or VisionX scanners currently configured with Firmware 1.2.1 or 1.5.1 can continue scanning in OTCnet without issue. However, in order to select the VisionX option in the terminal configuration scanner drop-down, Firmware 1.6.0 must be installed.
[5] Includes AGM Windows Vista Image

Please note that Offline users will not be able to use Firmware 1.6.0 unless they download the Release 1.5 Offline application. Furthermore, if you use the VisionX scanner on Firmware1.6.0, you must select VisionX from the drop- down menu. Users running Firmware1.6.0 with the MyVision X or VisionX scanners may receive two connectivity messages when clicking **Start Scan** after the first time the scanner USB is connected. Please accept the messages and re-click **Start Scan**. If the messages persist, please contact the Customer Support Team At 866-945-7920 or FMS.OTCChannel@citi.com.

The following keypads are compatible with OTCnet (KeyPads are optional hardware components – not required):

- Ingenico i3050
- Ingenico eN-Crypt[1]

[1]Ingenico encrypt was not tested for Release 1.5.Please note: USB-to-Serial adapters are not supported for any keypad device.

OTCnet Check Capture Offline Application Requirements

This section details the additional system and configuration requirements necessary to use OTCnet Offline, which is available for users performing check processing/check scanning in areas with low bandwidth and/or unreliable internet connectivity. **These requirements are only necessary for the OTCnet Offline Check Capture Application.**

Additional System Requirements

The following system requirements are necessary to use the OTCnet Offline.

- **Free Disk Space:** 600 MB additional disk space. 350 MB is required to install the application; 250 MB is recommended to accommodate transaction and audit log data.
- **Secondary Storage:** Secondary storage is required. It is recommended that an external hard drive or network drive is used instead of a local folder for storage on the individual Offline terminal. An external hard drive or network drive with 150 MB free disk space or USB flash drive is advised.
- **Java Access Bridge:** For 508 users, the Java Access Bridge must be installed on the workstation for Check Processing Offline to support the reading of a few browser pop-up windows. For 32-bit operating systems, JAWS 10 or higher must be used with Java Access Bridge 2.0.2 installed. For 64-bit operating systems, JAWS 13 must be used with Java Access Bridge 2.0.2 installed. Please click here for instructions on installing the Java Access Bridge: http://www.fms.treas.gov/otcnet/related.html#sys_req_4

- **Windows User Permissions**: OTCnet users must *not* have Windows administrator access to the workstation on which the Offline application is installed. In addition, all workstation users must have "write" permissions to the following subfolders within the Offline application's main installation folder:
    - C:\OTCnet_prod\data
    - C:\OTCnet_prod\log
    - C:\OTCnet_prod\server\logs

  All folders and subfolders within the main Offline application folder (except the three folders specified above) must be set to "read-only" permissions for all OTCnet users on the workstation. To ensure "read-only" permissions are set for the OTCnet root folder and its subfolders, apply the following permissions to the OTCnet root folder: "*Read & execute*", "*List folder contents*" and "*Read*", for all workstation users (typically applied for the "*Authenticated Users*" and "*Users*"/"Domain Users" groups on the workstation).

  To set "write" permissions for the three folders specified above, you must apply the "*Modify*", "*Read & execute*", "*List folder contents*", "*Read*" and "*Write*" permissions to the three folders for all workstation users (typically applied for the "*Authenticated Users*" and "*Users*"/"Domain Users" groups on the workstation).

  If upgrading OTCnet, set all OTCnet folders to "write", run the upgrade installer, then follow the above instructions to set the folder permissions accordingly.

  Failure to follow this requirement may result in application exploits for which agencies will have to assume responsibility.

- **McAfee Exclusion**: McAfee Antivirus users that experience slow application startup times are advised to implement the following exclusions based on the Operating System used at the terminal.
  Windows XP:
  C:\Documents and Settings*\Local Settings\Temp\jetty-0.0.0.0-XXXX-otcnet-offline.war-_otcnet-any-\
  C:\Documents and Settings*\Local Settings\Temp\JRCJNI\
  C:\OTCnet_prod\

  Windows 7:
  C:\Users*\AppData\Local\Temp*\jetty-0.0.0.0-XXXX-otcnet-offline.war-_otcnet-any-\
  C:\Users*\AppData\Local\Temp*\JRCJNI\
  C:\OTCnet_prod\

  Please note that the McAfee Exclusion C:\OTCnet_prod\ is based on the default install location for OTCnet. Users should apply the appropriate McAfee Exclusion above based on the install location of OTCnet selected during the installation process. During the installation process of OTCnet Offline, users have the option to select the location to install.

  Also, please note that users should apply the appropriate McAfee Exclusion above based on the Server HTTPS Port used in the OTCnet Offline installation process. During the installation process of OTCnet Offline, users have the option to input the Server HTTPS Port or keep the default Port setting. Please note the McAfee Exclusions above use the Server HTTPS Port XXXX, however users must use Port inputted during the installation process.

OTCnet Bandwidth Requirements

This section provides the minimum internet connectivity recommendations for setting up and utilizing OTCnet. Your agency's OTCnet Point of Contact (POC) has the Deployment Specialist's contact information, should you require assistance.

Bandwidth

- A 1.2 MB connection is recommended to download the OTCnet Scanner Firmware and/or the OTCnet Offline client
- A 512 KBPS DSL connection is recommended to utilize the OTCnet Online application
- A 512 KBPS DSL connection is recommended to utilize the OTCnet Offline application when uploading batches

Technical Reference Guide

This section provides further information to your agency system administrator on the system and configuration requirements needed for the online use of OTCnet. **Please note that the Check Scanning and Check Processing requirements are only necessary if OTCnet is used for check processing/check scanning.** Your agency's OTCnet Point of Contact (POC) has the Deployment Specialist's contact information, should you require assistance.

OTCnet General Requirements

- **Entrust Root Certificate:** Validate that the "Entrust 2048" Root Certificate is installed in the "Trusted Root Certification Authorities" store for all user profiles on the workstation. The full name on the certificate is "Entrust.net Certification Authority (2048)". The "Entrust 2048" Root Certificate is normally installed by default with Internet Explorer. If it has been removed, you will need to have your agency re-install the certificate, which can be obtained at: http://www.entrust.net/developer
- **Internet Options Security Settings**: "**Use TLS 1.0**" must be enabled in the advanced tab of Internet Options for all user profiles on the workstation. Multiple TLS (Transport Layer Security) versions may be available in your browser settings and at least one of these is normally enabled by default. You must ensure "**Use TLS 1.0**" is enabled in order to access both ITIM and OTCnet from the same browser.
- **Compatibility View or Browser Mode**: If using IE9, Compatibility View must be used or the Browser Mode must be set to IE8 when accessing OTCnet. To use Compatibility View in IE9, press the "Alt" key to toggle the menu bar (the menu bar includes the following top level menu items: **File**, **Edit**, **View**, **Favorites**, **Tools**, **Help**). Go to "Tools -> "Compatibility View settings" and add the "treas.gov" web site (without the quotes). To set the Browser Mode to IE8, press the F12 key, then click the "Browser Mode" tab near the bottom and select the "Internet Explorer 8" option. Because the Browser Mode defaults back to IE9 after closing the browser, it may be more convenient to use Compatibility View, which can applied specifically to OTCnet (i.e. "treas.gov") and does not have to be re-applied after closing the browser.

Check Scanning and Check Processing

- **OTCnet URL Added to Trusted Sites Zone:** You can use the Group Policy Object Editor or Group Policy Object Editor snap-in to add the OTCnet URL to the Trusted Sites Zone. This step is necessary to ensure ActiveX is enabled for OTCnet check scanning (ActiveX is typically enabled in the Trusted Sites Zone). Add the following OTCnet URL to the Trusted Sites Zone for all user profiles on the workstation: **https://www.otcnet.fms.treas.gov**
- **ActiveX must be enabled in browser:** If you cannot add the OTCnet URL to the Trusted Sites Zone, or if your organization does not enable ActiveX in the Trusted Sites Zone for your workstations, you will need to enable ActiveX in all Zones for all user profiles on each OTCnet workstation in order to support check processing. Use the following browser security settings to securely enable ActiveX:
    - Allow previously unused ActiveX controls to run without prompt -> **Disable**
    - Allow Scriptlets -> **Disable**
    - Automatic prompting for ActiveX controls -> **Disable**
    - Binary and script behaviors -> **Enable**
    - Display video and animation on a webpage that does not use external media player -> **Disable**
    - Download signed ActiveX controls -> **Prompt**
    - Download unsigned ActiveX controls -> **Disable**
    - Initialize and script ActiveX controls not marked as safe for scripting -> **Disable**
    - Only allow approved domains to use ActiveX without prompt -> **Enable** (IE 8 only)
    - Run ActiveX controls and plug-ins -> **Enable**
    - Script ActiveX controls marked safe for scripting -> **Enable**
- **ActiveX Filtering must be disabled in browser (IE9 only):** If using IE9 (in Compatibility View or Compatibility mode), the "ActiveX Filtering" option must be disabled (unchecked) in the "Tools" menu in the browser. Ensure this is disabled by going to the "Tools" menu from the menu bar and confirming that the "ActiveX Filtering" menu option is unchecked. Note that the "Alt" key toggles the menu bar in IE9. Alternatively, click the "gear" (i.e. "tools") icon in IE9, then go to the "Safety" menu item and ensure that "ActiveX Filtering" is unchecked.
- **Scanner Drivers (.MSI installation file):** Scanner driver and Firmware (provided in an .MSI installation file) must be installed on the workstation. Instructions for obtaining and installing the .MSI file can be found in the OTCnet Web Based Training, Module 6.3: Download Firmware.

For More Information

To learn more about OTCnet, please access our website at: http://www.fms.treas.gov/otcnet/index.html, email us at fms.otcdeployment@citi.com or call 703-377-5586.